INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A., Google Scholar, Indian Citation Index (ICI), J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)], Index Copernicus Publishers Panel, Poland with IC Value of 5.09 (2012) & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than **7835 Cities** in **197 countries/territories** are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to the recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____________

THE EDITOR

IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF** ____.

(e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript titled '____' for likely publication in one of your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published anywhere in any language fully or partly, nor it is under review for publication elsewhere.

I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to inclusion of their names as co-authors.

Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation/Post*	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

* i.e. Alumnus (Male Alumni), Alumna (Female Alumni), Student, Research Scholar (M. Phil), Research Scholar (Ph. D.), JRF, Research Assistant, Assistant Lecturer, Lecturer, Senior Lecturer, Junior Assistant Professor, Assistant Professor, Senior Assistant Professor, Co-ordinator, Reader, Associate Professor, Professor, Head, Vice-Principal, Dy. Director, Principal, Director, Dean, President, Vice Chancellor, Industry Designation **etc**. ***The qualification of author is not acceptable for the purpose***.

NOTES:

a) The whole manuscript has to be in ***ONE MS WORD FILE*** only, which will start from the covering letter, inside the manuscript. ***pdf. version* is liable to be rejected without any consideration**.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of the mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) Only the **Abstract will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) ***The journal gives acknowledgement w.r.t. the receipt of every email within twenty-four hours*** and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of the manuscript, within two days of its submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except on the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE:** The title of the paper should be typed in **bold letters**, **centered** and **fully capitalised**.
3. **AUTHOR NAME (S) & AFFILIATIONS:** Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.
4. **ACKNOWLEDGMENTS:** Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.
5. **ABSTRACT:** Abstract should be in **fully Italic printing**, ranging between **150** to **300 words**. The abstract must be informative and elucidating the background, aims, methods, results & conclusion in a **SINGLE PARA**. ***Abbreviations must be mentioned in full***.
6. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations etc.
7. **JEL CODE:** Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php. However, mentioning of JEL Code is not mandatory.
8. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. *It should be free from any errors i.e.* ***grammatical, spelling*** *or* ***punctuation.*** *It must be thoroughly edited at your end*.
9. **HEADINGS:** All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.
10. **SUB-HEADINGS:** All the sub-headings must be bold-faced, aligned left and fully capitalised.
11. **MAIN TEXT:**

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably be in ***2000 to 5000 WORDS***, But the limits can vary depending on the nature of the manuscript.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self-explained, and the **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text*.
13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, left aligned with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word may be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.
14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section e.g. Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.
15. **REFERENCES:** The list of all references should be alphabetically arranged. ***The author (s) should mention only the actually utilised references in the preparation of manuscript*** and they may follow Harvard Style of Referencing. **Also check to ensure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc., in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italic printing. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parenthesis.
- ***Headers, footers, endnotes*** *and* ***footnotes*** *should* ***not be used*** *in the document****.*** However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders before the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

A GENETIC ALGORITHM BASED IMAGE AUTHENTICATION TECHNIQUE FOR DIGITAL IMAGE USING PIXEL VALUE DIFFERENCING (GASTPVD)

Dr. AMRITA KHAMRUI
ASST. PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE
VIVEKANANDA COLLEGE
MADHYAMGRAM

ABSTRACT

In this paper Genetic Algorithm based steganographic technique for digital image using pixel value differencing (GASTPVD) has been proposed. This is a spatial domain-based image authentication technique where correlation between the neighboring pixels determines the number of secret bits to be embedded. The difference between consecutive two pixels in the edge area is larger than the difference between the consecutive two pixels in smooth areas. So, more number of secret bits can be embedded in edge area than smooth area. In this proposed technique variable number of secret bits can be embedded based on the difference(d) between consecutive two pixels. The difference between consecutive two pixels has been categorized into four area as follows: very smooth, smooth, medium smooth and edge area. If d <= 31, then difference fall into very smooth area. If 31<d<= 63, then difference fall into smooth area. If 63<d<= 127, then it falls into medium smooth area. If d>127, then it falls into edge area. Three, four, five and six secret bits are embedded in the very smooth, smooth, medium smooth and edge area difference respectively. Genetic Algorithm has been applied to generate optimized stego image. The proposed technique has been compared with two existing pixel value differencing based steganographic techniques. It shows that the proposed technique performs better than existing approach.

KEYWORDS

genetic algorithm (GA), image fidelity (IF), peak signal to noise ratio (PSNR), pixel value difference (PVD), mean square error (MSE).

JEL CODE

O31

1. INTRODUCTION

Steganography is the concealment of digital information in the form of image/ video/ text within computer files/images. The covering image is also named as source image. The information that is hidden in the cover image [18],[23] is referred to as secret information. The cover image with secret information hidden on it is referred to as stego image [6]. Steganography [4] means embedding of digital information within computer files/images. In General, secret information in steganography can be anything, it may be video, image [9],[10], sound file even the radio communication also. To ensure security, a message may be secretly embedded by using some algorithms [5] which is invisible to the intruder and also reversible [8] as the message can be extracted from the receiver end. Security [13], [15] may be achieved by hiding message/ image within an image either in spatial domain [14] or in frequency domain. Image authentication can be achieved through data hiding technique [11], [12]. Ownership verification is an important task of military people. Authentication [16], [17] is the major task for research institute and scientist. Ownership verification and image authentication [22] has become very important to secure the document from unauthorized access. Steganography means secret communication within a host image and the secret communication can be message, image, and video. A popular example of steganography is that of a prisoner secretly communicating with outside under the supervision of a prison warden. Steganography is useful method to the construction of a hypermedia document or image, which is very less convenient to manipulate. The objective of steganography or data hiding is to hide the message/image in the source image by some key techniques and cryptography [19] hides the message content. In case of steganography, a message is hidden inside a cover image without changing its visible properties [7] and the content of source image can be changed. A popular method of steganography is least-significant bit (LSB) substitution developed by [7] masking, filtering and transformations on the source image. All the experiments have been performed on the image taken from the image database [20].

Rest of the paper is organized as follows. Section 2 deals with review of literature. Section 3 deals with importance of the study. Section 4 deals with the statement of the problem. Section 5 discuss the objective of the proposed technique. Section 6 discuss the hypothesis. The research methodology has been discussed in section 7. Results and discussion are discussed in section 8. Some findings are mentioned in section 9. Recommendations are given in section 10. Conclusion, limitation and scope for future research are presented in section 11, 12 and 13. References are drawn at end.

2. REVIEW OF LITERATURE

Some existing methodologies has been discussed in this section. In 2021, Fadhel S A et al.[1] proposed an improved “pixel-value differencing” steganographic method that uses AES method to encrypt and hide the important text data. This method builds a map to embed in non-sequential way by using hyperchaotic system that increases the security level. In this technique data embedding is done one of the three levels of the colour image that is Red or Green or Blue. This increases the efficiency of this technique. In 2020, Kim P H et al.[3] proposed another dual image based pixel-value differencing technique which is reversible in nature. This technique can hide more number of secret information based on neighbouring pixel difference. In this technique non-overlapping mask is taken from the source image and the difference between the neighbouring pixels are calculated. The highest difference is chosen for embedding. A hash function is taken for determining the number of secret bits. In 2020 Majumder J et al.[2] proposed a steganography technique based on Pixel Value Difference and some cryptographic method such as AES and SHA-2. It combines cryptography with steganography. Here a message is encrypted using AES algorithm using SHA-2 as hash function. Pixel value differencing technique has been used by adding a key to the hash function. Another pixel value differencing steganography technique proposed by Majumder J [4] in 2020 based on neighbouring pixel matching. It is a reversible data hiding scheme which considers two, three and four neighbouring pixels. It embeds a greater number of bits in edge areas than smooth areas as the edge area can tolerate more changes than smooth areas. In 2017 Al Dhamari A K et al. [5] proposed pixel value differencing-based steganography technique which uses new structure of blocks to hide secret information. It also uses modulus function as a hash function. In 2016 Jana B et al. [7] proposed reversible data hiding technique for dual-image. It is a pixel value differencing technique where secret information is divided into two sub-streams. First hides n-1 bits secret data using pixel value differencing technique, next hide 1 bit using difference expansion for n bit secret data. It uses two neighbourhood pixels for calculating the difference. Another technique proposed by Jana B et al. [6] is dual image-based steganography using pixel value differencing and exploiting modification direction. The secret information is embedded using two ways, some bits are embedded using pixel value differencing technique and some are embedded using exploiting modification direction in pair of pixels. The modified pixel pairs are distributed among the dual images. This method obtained two modified pairs of pixels which contain 7 bits secret message and distributed these pixel pairs among dual stego images depending on a shared secret key (K). The recipient successfully obtains secret message and retrieve original image using same shared secret key.

3. IMPORTANCE OF THE STUDY

The existing techniques used different steganographic techniques but the amount of secret information is not so much. This paper presents an algorithm that would facilitate secure message transmission using mask-based data hiding procedure depends on pixel value differencing technique. This method embeds large amount of secret information as compared to the existing works [4],[5],[6],[21] with minimum distortion of visual property as it embeds more bits in the edge area compared to the smooth area. The proposed method GASTPVD is compared with other existing techniques and find out good results with respective to payload as the edge areas can tolerate more changes than the smooth areas.

4. STATEMENT OF THE PROBLEM

The detailed study of the Review of Literature reveals the following facts:
Most of the previous techniques are LSB substitution techniques but in the proposed technique variable amount of information are embedded based on the difference. Few techniques used Genetic Algorithm as the optimization process to generate optimized stego image but in this technique, GA is used as optimization technique. Most of the earlier works used less embedding capacity but the proposed techniques conform large embedding capacity with least distortion in the stego image.

5. OBJECTIVE

The objective of this research is to develop a new Genetic Algorithm based image authentication technique that can hide large message by keeping quality stego image.

6. HYPOTHESIS

The proposed technique uses some benchmark images taken from the USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering [20]. Source and authenticating images are considered as color images.

7. RESEARCH METHODOLOGY

In GASTPVD, a mask of size 2×2 from the source image [20] is taken in row major order. Another image is taken as the authenticating image from the image database [20]. First four mask is used for embedding dimension of the authenticating image. Authenticating image dimension is extracted from the header part of the image and is embedded in the first four mask of the source image with a bit per byte (bpb) of 3. The dimension is embedded in the rightmost three LSB position. Authenticating image pixels are embedded through pixel value differencing technique using 2-neighbour pixel. The difference value (d) has been calculated by the difference between the two neighbour pixels. According to the difference value (d) four areas are determined. Those are very smooth area, smooth area, medium smooth area and edge area. If the difference value(d) is less than or equal to 31, then it falls into very smooth area and three bits from the authenticating image are embedded in the difference value. If the difference value(d) falls between 31 and 63, then it falls into smooth area and four bits from the authenticating image are embedded in the difference. If the difference value(d) falls between 63 and 127, then it falls into medium smooth area and five bits are embedded in the difference. If the difference value(d) is higher than 127, then it falls into edge areas and six bits are embedded in the difference. The pixel value differencing method is a reversible steganographic technique that embed more number of bits in the edge area compared to the number of bits in the smooth area using the high correlation among the pixels. If the pair of adjacent pixels are X_1 and X_2, the difference value d is calculated by the **equation (1)** and mean value m is calculated through **equation (2)**. The inverse transform is given by **equation (3)** and **equation** (4).

$d = X_1 - X_2,$ (1)

$m = floor((X_1+X_2)/2$ (2)

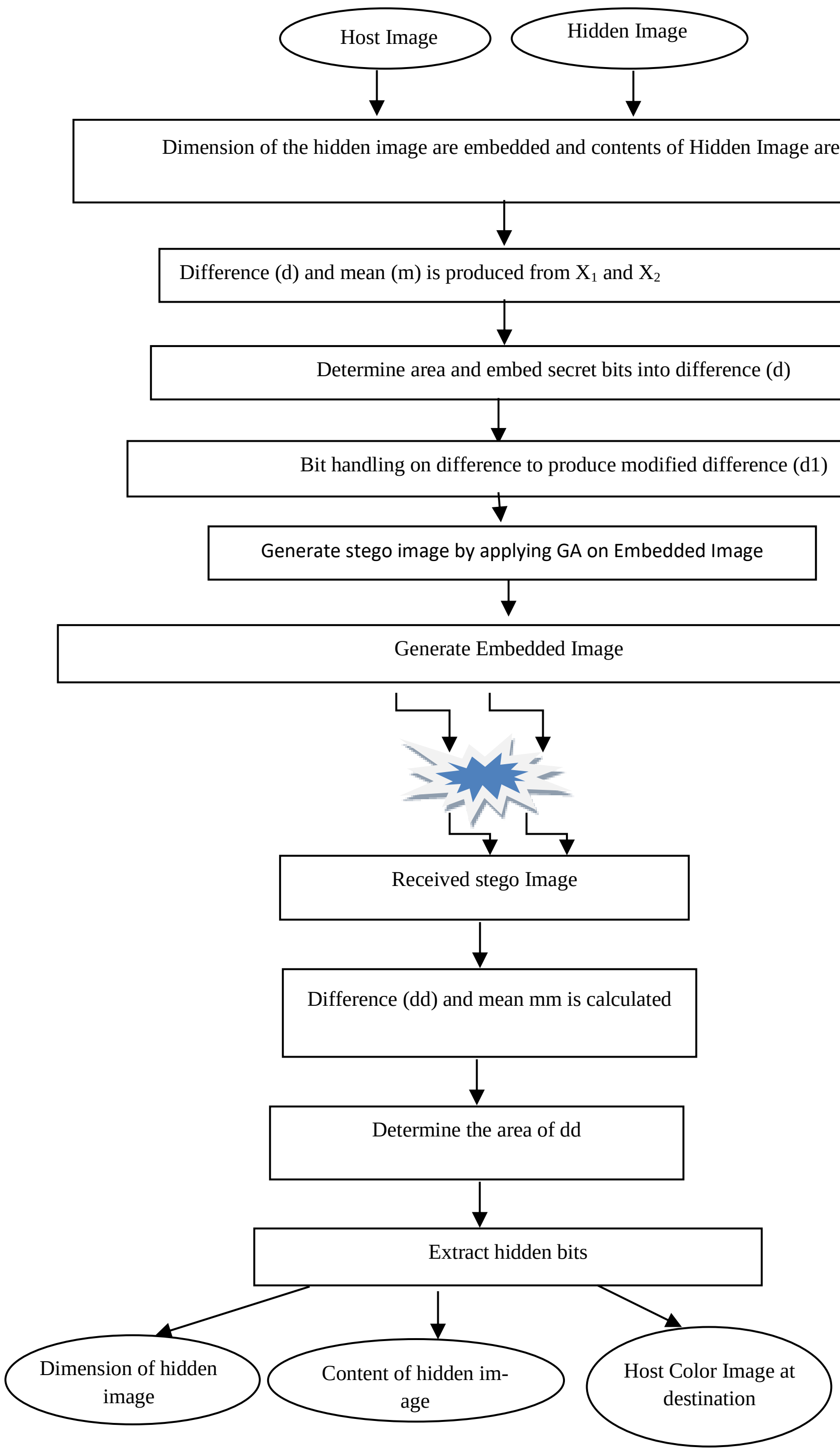
$X_1 = m + floor((d+1)/2)$ (3)

$X_2 = m - floor(d/2)$ (4)

The difference value (d) determines the number of authenticating image bits to be embedded on it. The induced distortion in the embedded image pixels is generated through the embedding of secret information on the difference value(d). A bit handling procedure has been introduced to keep the embedded difference value in the same area (very smooth/ smooth/ medium smooth/ edge area) to ensure the reversibility. The modified pixel values (X_{11} and X_{22}) are generated through the equation (3) and (4). Embedded stego image is processed through Genetic Algorithm to generate optimized stego image. The optimized stego image is transmitted through network. At the receiver end optimized stego image is received. The authenticating image bits are extracted using extraction algorithm. The algorithm of insertion is discussed in section 7.1 and the algorithm for extraction is discussed in section 7.2.

Schematic diagram of the technique discussed above is shown Figure 1.

FIGURE 1: SCHEMATIC DIAGRAM OF GASTPVD



7.1 ALGORITHM FOR INSERTION

Input: Source image is of dimension 512×512, secret authenticating image is of dimension 256 × 256.

Output: embedded image having dimension 512×512.

Steps:

1. Source image mask of 2×2 is taken.
2. The dimension of the authenticating image is extracted.
3. Calculate the difference (d) between the two neighbours.
4. Find out the area in which the difference (d) belongs and embed secret information on the difference (d). If the area changes, then use bit handling method to make the difference in the same area to keep reversibility.
5. Use the equation (3) and (4) to generate the embedded pixel value.
6. Apply GA to generate the optimized stego image. The process of GA has been discussed in section 7.1.1.

The insertion algorithm is illustrated with one example in figure 2.

FIGURE 2: INSERTION OF THE AUTHENTICATING IMAGE BITS IN THE SOURCE IMAGE MASK

10110000 01010000 Figure 2a: Authenticating image pixels	226 137 157 219 Figure 2b: Source image Lenna	01011001 00111110 Figure 2c: Difference image block
01001101 00110000 Figure 2d: Embedded difference image block	220 143 212 164 Figure 2e: Embedded image block	220 143 212 164 Figure 2f: Embedded image block after bit handling

In the figure 2a authenticating image pixels are shown in binary form. The source image pixels are shown in Figure 2b. Here Lenna image from image database [20] has been taken as the source image. The difference between the two neighbour is shown in figure 2c. The difference is in medium smooth region. So, 5 bits from the authenticating image are embedded in the difference shown in Figure 2d. Embedded image pixels are shown in Figure 2e with the help of equation 3 and equation 4. As the region is not changed, so the bit handling process results the same as embedded image pixels and is shown in Figure 2f.

7.1.1 PROCESS OF GENETIC ALGORITHM

Input: embedded image is of size 512×512.
Output: optimized stego image is of size 512×512.
Steps:

1. A 2 × 2 mask from the embedded image is taken.
2. Initial population is considered for the two neighbours of the mask (explained in initialization section).
3. The selection process uses Roulett Wheel selection to select the two fittest chromosomes from the initial population.
4. Crossover is performed over the two fittest chromosomes (explained in section crossover). Crossover results two children.
5. Result of Crossover are processed through mutation (explained in mutation section).
6. The process of elitism (explained in elitism section) and process of termination (explained in termination section) are applied at last.
7. Step 1 to 6 is repeated for the entire matrix.
8. Step 1 to 7 is repeated for the entire embedded image.

Initialization

In Initialization random pixel value has been generated which are less than or equal to 255. The maximum number of authenticating image bits can be embedded per byte is three, so 2^3 that is 8 number of random chromosomes are generated for each pixel in the mask.

Selection

In this process fittest chromosomes are selected using Roulett Wheel selection process with the help of the fitness function

$f(n) = 1/(mod(s(x,y) – c(x,y))+1)$

f(n) is the fitness function, s(x,y) is intensity value of stego image pixel for the coordinate (x, y). c(x, y) is intensity value of Host image/ source image for the same coordinate (x, y).

Crossover

Two fittest chromosomes for each neighbour are selected through selection process passed through crossover. Uniform crossover process is followed where first bit is from first parent and second bit is from second parent. Example shows the crossover for a pixel of the two neighbours.

Parent 1 = 191

1	0	1	1	1	1	1	1

Parent 2 = 223

1	1	0	1	1	1	1	1

Offspring1 = 255

1	1	1	1	1	1	1	1

Offspring2 = 159

1	0	0	1	1	1	1	1

Mutation

Mutation is applied on the cross overed chromosomes for each neighbour by taking a bitwise XOR on the last three bits on three steps and taking the first bit of each step. Mutation process is explained below for one of the two neighbours.

Before Mutation=255

1	1	1	1	1	1	1	1

After Mutation=252

1	1	1	1	1	1	0	0

Elitism

Elitism forwards the best chromosomes in the next iteration by eliminating the weak chromosomes. In this case by calculating the difference value of two neighbours it forward the two best chromosomes in the next iteration. If the difference value of two mutated chromosomes are same as the difference value of two embedded chromosomes then it forward the result to the next iteration otherwise pass the old value to the next iteration.

7.2 EXTRACTION ALGORITHM

Input: Optimized stego image having dimension 512×512.
Output: Secret authenticating image having dimension 256×256.
Steps:

1. An image mask of size 2 × 2 is taken from the optimized stego image.
2. Calculate the difference between the consecutive two neighbours of the mask.
3. Find out the region in which the difference belongs to and extract the authenticating image bits according to the region.
4. 8 bits extraction form a byte of the authenticating image.
5. Repeat step 1 to 4 according to the dimension of the authenticating image.

Decoding Correctness

The proposed technique embeds the authenticating image pixels in the difference of two neighbours, and GA has been applied to generate optimized stego image. So, the difference between the two neighbours should be same after the generation of optimized stego image, otherwise the extraction of authenticating image bits will not be possible. This is ensured in the elitism step of GA. For example, if the difference between the consecutive two pixels after embedding is 232 and 104, after applying GA, if must be accepted if the values are 236 and 108. That means the difference value should be same to keep the decoding properly.

8. RESULTS AND DISCUSSION

The results are generated on Intel Core 2 Duo CPU having 3.00 GB RAM and 2.00GHz speed. Source images are of dimension 512 × 512 and authenticating image is of size 256 × 256. Table 1 shows the experimental results performed on GASTPVD for the following image metrices like PSNR, MSE, IF and SSIM shown in equation (5), (6) (7) and (8). PSNR is peak signal to noise ratio measured in decibels between two images. PSNR is used to find out the quality of the stego image as compared to the source image. Higher value of PSNR ensures better quality of the stego image. MSE is mean square error is used to compare the quality of the stego image as compared to the source image. MSE measures the cumulative squared error between the stego image and the source image. The lower value of MSE ensures the lower error. IF is image fidelity used to discriminate between two images how accurate those are. If the two images are same then IF will be 1. SSIM refers to structural similarity index measurement is obtained by comparing the pixel intensities. It is another metric for comparing the image degradation due to information hiding. If two images are same it will be 1. The formula for SSIM is given in equation (8), where the formula for μ_x and μ_y is given in equation (9) and σ_x^2 and σ_y^2 are given in equation (10) and (11). The formula for σ_{xy} is given in equation (12) and the constants C_1, C_2, K_1, and K_2 are given in equation (13).

The experimental results for all the sixteen images (Table 1) have been observed that the PSNR value lies between 42 and 49 which results better quality of the stego image. The highest PSNR is 48.209309, lowest PSNR value is 42.121918. IF value lies between 0.999628 and 0.999975. The highest value of IF is 0.999975 and the lowest value of IF is minimum value 0.999628 which results stego image is almost same as source image. MSE value indicated that how close the source image with stego image. Lower value of MSE (ranging from 0.873201 to 3.989226) in the table indicates that the stego image and source image are very close. SSIM value is very closer to 1 which indicates that the optimized stego image is almost same as source image. Figure 3 shows the visual interpretation of various source and optimized stego images. It is seen that there are no such visual changes in the source and optimized stego image. Table 2 shows the comparison of existing technique with the proposed technique. It has been observed that the proposed technique embeds more volume of secret information than the existing methodologies[2] and a better quality of image as compared to the existing methodology[3]. It has also noted that the proposed technique obtains high PSNR value as compared to the existing methods. It means that the quality of the optimized stego image is better than the existing methodologies.

$$PSNR = 10\,\log\left(max\left(I_{m,n}{}^2\right)/MSE\right) \quad (5)$$

$$MSE = \frac{1}{MN} * \sum_{m,n} (I_1\, m,n - I_2 m,n)^2 \quad (6)$$

$$IF = 1 - \sum_{m,n} (I_{1_{m,n}} - I_{2_{m,n}})^2 \,/\, \sum_{m,n} I_{2_{m,n}}^2 \quad (7)$$

$$SSIM = 2(\mu_x\mu_y + C_1)(2\sigma_{xy}+C_2)/((\mu_x * \mu_x + \mu_y * \mu_y + C_1) * (\sigma_x * \sigma_x + \sigma_y * \sigma_y + C_2) \quad (8)$$

$$\mu_x = 1/N \sum_{i=1}^{N} X_i,\ \mu_y = 1/N \sum_{i=1}^{N} Y_i \quad (9)$$

$$\sigma_x * \sigma_x = 1/N\text{-}1 \sum_{i=1}^{N} (X_i - \mu_x)^2 \quad (10)$$

$$\sigma_y * \sigma_y = 1/N\text{-}1 \sum_{i=1}^{N} (Y_i - \mu_y)^2 \quad (11)$$

$$\sigma_{xy} = 1/N\text{-}1 \sum_{i=1}^{N} (X_i - \mu_x)(Y_i - \mu_y) \quad (12)$$

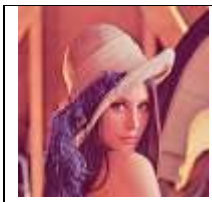
The value of C_1, C_2 and C_3 with K_1 and K_2 are from [23] given in equation (13)

$$C1 = (K_1\, L)^2,\ C2 = (K_2\, L)^2,\ K1 = 0.01,\ K2 = 0.03 \quad (13)$$

TABLE 1: PSNR, MSE, IF AND SSIM VALUES OF VARIOUS OPTIMIZED STEGO IMAGES

Cover image	*PSNR*	*MSE*	*IF*	*SSIM*
Lenna	43.434471	2.948718	0.999852	0.999996
House	46.716660	1.384888	0.999949	0.999999
Baboon	45.350311	1.896921	0.999901	0.999999
Pelican	46.895218	1.329103	0.999961	0.999998
Pepper	43.178005	3.128094	0.999812	0.999998
Peaceful	46.867504	1.337611	0.999858	0.999999
Avion	48.719662	0.873201	0.999975	0.999768
Toucan	42.977612	3.275814	0.999740	0.993818
Tahoe	44.771507	2.167352	0.999733	0.999561
Sailboat	45.660923	1.765990	0.999911	0.995216
Manhatan	48.209309	0.982086	0.999908	0.999999
Sedona	46.864376	1.338575	0.999871	0.999703
Colomtm	46.542160	1.441664	0.999887	0.999999
Butrfly1	45.932850	1.658806	0.999887	0.999916
Blueeye	45.163162	1.980451	0.999628	0.999999
Blakeyed	42.121918	3.989226	0.999646	0.999999

FIGURE 3: VISUAL INTERPRETATION OF VARIOUS SOURCE AND OPTIMIZED STEGO IMAGES


i. Source image lenna

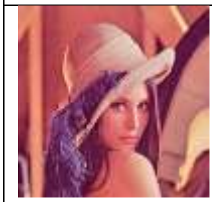

ii. Source image baboon


iii. Source image pepper


iv. Source image tahoe


v. Source image toucan


vi. Authenticating image jet


vii. Optimized stego lenna


viii. Optimized stego baboon


ix. Optimized stego pepper


x. Optimized stego tahoe


xi. Optimized stego toucan

TABLE 2: COMPARISON OF PSNR VALUES AND THE CAPACITY OF VARIOUS OPTIMIZED STEGO IMAGES WITH EXISTING APPROACH

Source image	PSNR value of existing technique[2]	PSNR value of existing technique[3]	PSNR value of GASTPVD	Capacity (in bytes) of existing technique[2]	Capacity (in bytes) of existing technique[3]	Capacity (in bytes) of proposed technique
Lenna	42.2	41.9185	43.434471	20480	100000	54000
Baboon	40.2	-	45.350311	21440		54000
Pepper	-	41.6474	43.178005		100000	54000

9. FINDINGS

It has been observed that the proposed technique having high PSNR value and IF value nearly equals to 1 which ensures good quality of the stego image and also embed large amount of secret information.

10. RECOMMENDATION

The proposed technique can be finding applications in the following areas:

This technique (GASTPVD) can be used in Image authentication. The image that needs to be authenticated is considered as source image. Another small image can be taken as authenticating image. Authenticating image is embedded using this approach and send across the network by keeping the visibility of the source image intact. At the receiver end it is extracted by the receiver using extraction algorithm. If the extracted image and the original authenticating images are same, then the image is authentic.

The proposed technique can be used in telemedicine. Telemedicine refers to the way of remote medical services via real time both way communication between patient and the doctor using audio or visual electronic means. If the image is communicated over the transmission media, then it should be authenticated. The process of authentication is stated in previous example. So GASTPVD can be used in image authentication.

GASTPVD can be used in document authentication. Consider a legal image. It consists of an image part and a text part. If someone tampers the document it can be recognized through GASTPVD. From the text part a digest can be generated using any message digest algorithm and it can be embedded in the image part of the legal document. When it needs to be authenticated the digest is extracted from the image part of the legal document and another digest is generated from the text part of the legal document. If both are same then the legal document is authenticated.

Bank can use secure e-payment method through steganography. Now a days there is huge demand of online shopping. This required online transaction. So, there is an important task to protect the customers information. GASTPVD technique can be used in this purpose.

GASTPVD can be used to hide the health record electronically for smart city application.

GASTPVD can be used for secure message transmission. The message that is to be transmitted in secure way should be hidden in the source image and can be transmitted over network. At the receiver end it is extracted from the transmitted image in reverse way.

11. CONCLUSION

The technique GASTPVD is a spatial domain colour image authentication technique based on pixel value differencing technique. This approach hides large amount of information with a little distortion and by applying Genetic Algorithm the quality of the optimized stego image is maintained. This technique has been compared with some existing pixel value differencing-based approaches and the result shows that the technique works better than those approaches.

12. LIMITATION

The proposed technique is a spatial domain technique. It cannot be applicable in frequency domain.

13. SCOPE FOR FUTURE RESEARCH

The capacity of the secret information can be increased in the proposed technique and hence future scope of research.

REFERENCES

1. Fadhel S A et al. “An Improved Data Hiding using Pixel Value Difference Method and Hyperchaotic System” Journal of Physics: Conference Series 1879 (2021) 022089, IOP Publishing doi:10.1088/1742-6596/1879/2/022089.
2. Majumder J “Neighbouring Pixel Matching Pixel Value Differencing Based Image Steganography”, Turkish Journal of Computer and Mathematics Education Vol.11 No. 01 (2020), 560-566.
3. Kim P H et al. “Reversible data hiding scheme based on pixel-value differencing in dual images”, International Journal of Distributed Sensor Networks 2020, Vol. 16(7) The Author(s) 2020 DOI: 10.1177/1550147720911006 journals.sagepub.com/home/dsn.
4. Majumder J et al. “Pixel Value Differencing Based Image Steganography using AES and SHA-2 Cryptography Method”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020.
5. Al-Dhamari A K et al. “Block-Based Steganographic Algorithm Using Modulus Function and Pixel-Value Differencing”, Journal of Software Engineering and Applications, 2017, 10, 56-77 http://www.scirp.org/journal/jsea ISSN Online: 1945-3124 ISSN Print: 1945-3116.

6. Jana B et al. “Dual-Image Based Reversible Data Hiding Scheme Through Pixel Value Differencing with Exploiting Modification Direction” J.K. Mandal et al. (eds.), Proceedings of the First International Conference on Intelligent Computing and Communication, Advances in Intelligent Systems and Computing 458, DOI 10.1007/978-981-10-2035-3_56, © Springer Science+Business Media Singapore 2017.
7. Jana B et al. “Dual-Image Based Reversible Data Hiding Scheme Using Pixel Value Difference Expansion”, International Journal of Network Security, Vol.18, No.4, PP.633-643, July 2016.
8. Giri D et al. “Dual Image Based Reversible Data Hiding Scheme Using Three Pixel Value Difference Expansion”, S.C. Satapathy et al. (eds.), Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing 434, DOI 10.1007/978-81-322-2752-6_40, © Springer India 2016.
9. T.C. Lu, C.Y. Tseng, and J.H. Wu, Dual Imaging-based Reversible Hiding Technique Using LSB Matching, Signal Processing, vol. 108, pp. 77–89, (2015).
10. Lu, Tzu-Chuen, Jhih-Huei Wu, and Chun-Chih Huang. Dual-image-based reversible datahiding method using center folding strategy. Signal Processing 115, pp. 195–213, (2015).
11. C. F. Lee, C. C. Chang, P. Y. Pai, and C. M. Liu, “Adjustment hiding method based on exploiting modification direction”, International Journal of Network Security, vol. 17, no. 5, pp. 607–618, 2015.
12. C. Qin, C.C. Chang, and T.J. Hsu, Reversible Data Hiding Scheme Based on Exploiting Modification Direction with Two Steganographic Images, Multimedia Tools and Applications, pp.1–12, (2014).
13. Jung K H et al. “Three-directional data hiding method for digital images” Article in Cryptologia · April 2014 DOI: 10.1080/01611194.2014.885817.
14. Chin-Feng Lee, Yu-Lin Huang, Reversible data hiding scheme based on dual stegano-images using orientation combinations, Telecommun Syst, vol. 52, pp. 2237–2247, (2013).
15. C.C. Chang, T.C. Lu, G. Horng, Y.H. Huang, and Y.M. Hsu, A High Payload Data Embedding Scheme Using Dual Stego-images with Reversibility, Proceedings of Third International Conference on Information, Communications and Signal Processing, pp. 1–5, (2013).
16. Ghoshal N., Mandal, J. K. et al., “Masking based Data Hiding and Image Authentication Technique (MDHIAT)”, proceedings of 16th International Conference of IEEE on Advanced Computing and Communications ADCOM-2008, ISBN: 978-1-4244-2962-2, December 14-17th, Anna University 2008.
17. Nameer N. EL-Emam, “Hiding a large Amount of data with High Security Using Steganography Algorithm,” Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.
18. C. Rechberger, V. Rijman and N. Sklavos, “The NIST cryptographic Workshop on Hash Functions,” IEEE Security and Privacy, vol. 4, pp. 54-56, Austria, Jan-Feb 2006.
19. Ghoshal N., Mandal, J. K. “A Novel Technique for Image Authentication in Frequency Domain using Discrete Fourier Transformation Technique (IAFDDFTT)”, Malaysian Journal of Computer Science, ISSN 0127-9094, Vol. 21, No. 1, pp. 24-32, 2008.
20. Allan G. Weber, The USC-SIPI Image Database: Version 5, Original release: October 1997, Signal and Image Processing Institute, University of Southern California, Department of Electrical Engineering. http://sipi.usc.edu/database/ (Last accessed on 20th January, 2011).
21. J K Mandal and A Khamrui, “A Data Embedding Technique for Gray Scale Image Using Genetic Algorithm (DEGGA)” (SP_2011_2001), IEEE sponsored International Conference on communication, computing & security (Proceedings by Excel India Publishers ISBN-978-93-80697-505), NIT Rourkela, 7-9 Jan,2011,pp.19-22,2011.
22. H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacement methods,” Proc. Inst. Elect. Eng., Vis. Images Signal Process., vol. 152, no. 5, pp. 611–615, 2005.
23. Mandal Jyotsna Kumar “Reversible Steganography and Authentication via Transform Encoding”, Studies in Computational Intelligence 901, Springer Nature.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue, as well as on the journal as a whole, on our e-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our e-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward to an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals